Notice of Allowability	Application No.	Applicant(s)	
	10/649,855	SUNDARAM ET AL.	
	Examiner	Art Unit	
	Aubrey H. Wyszynski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/26/03*.

2. ☒ The allowed claim(s) is/are *1-10*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 2/4/04, 8/26/03
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

DETAILED ACTION

1. Claims 1-10 are pending.

Allowable Subject Matter

2. Claims 1-10 are allowed.

3. The following is a statement of reasons for the indication of allowable subject matter:

4. Regarding claim 1:

Gennaro et al, U.S. Patent No. 6,292,897 discloses authenticating a digital signature comprising:

- generating two prime numbers p and q (col. 3, lines 52-53)
- generating public and private keys, the signing algorithm (fig. 1, #120) used to generate signature S, computed by raising the message M to the secret power d as $S= M^d \bmod n$ (col. 3 lines 59-63)
- receiving public verification key VK (fig. 1, #110)
- and validating the signature if $M'=S'^e \bmod n$, holds true (col. 4, lines 1-4).

5. Gennaro fails to teach a publicly known generator is alpha such that alpha.sup.q.ident.1 (mod p), providing an order list of public keys, selecting uniform at random by a prover a non-negative number r less than q, sending a number x=alpha.sup.r (mod p) from the prover to a verifier; selecting uniformly at random, by the verifier, a non-negative number e less than 2.sup.(t+logd), where log is base 2, and a number t is a predetermined security parameter; receiving by the prover from the verifier the number e; generating, by the prover, a number y=r+.SIGMA..sub.i s.sub.i*e.sup.i

(mod q); sending by the prover to the verifier the number y; determining if an equality x=.alpha..sup.y*.PI..su- b.i(v.sub.i).sup.e.sup..sup.i (mod p) is true; and accepting the prover as having the d.sub.i identities if and only if the equality is true.

6. Independent claim 1 identifies distinctive features of generating, by the prover, a number y=r+.SIGMA..sub.i s.sub.i*e.sup.i (mod q); sending by the prover to the verifier the number y; determining if an equality x=.alpha.sup.y*.PI.sub.i(v.sub.i).sup.e.sup..sup.i (mod p) is true; and accepting the prover as having the d.sub.i identities if and only if the equality is true. The closest prior art, Generro teaches authenticating identies using two prime numbers p and q, including a public key and a private key and a random generator signature. The cited prior art fails to teach generating, by the prover, a number y=r+.SIGMA..sub.i s.sub.i*e.sup.i (mod q) and determining if an equality x=.alpha..sup.y*.PI..sub.i(v.sub.i).sup.e.sup..sup.i (mod p) is true and thus fails to anticipate or render the above limitations obvious. For these reasons independent claim 1 and dependent claims 2-10 have been found allowable.

7. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Goldwasser et al., U.S. Patent No. 4,926,479 discloses a multiparty verification system consisting of a prover and a verifier coupled to process respective outputs to provide identification and verification.

b. Girault et al, U.S. Patent No. 7,184,547 discloses using the zero-knowledge protocol to verify a relation ship between and prover possessing a public key and a verifier, which knows the public key.

c. Brands, U.S. Patent No. 5,606,617 discloses enable forming and issuing of secret key certificates.

d. Brickell et al., U.S. Patent No. 5,867,578 discloses a distributed root certifying authority.

e. Hoffstein et al., U.S. Patent No. 6,959,085 and U.S. Patent No. 6,076,163 disclose authenticating an identity using challenge communication and verification.

f. Kim et al. U.S. Patent Application Publication No. 2004/0064700 discloses a method for identification using a private and public key and random numbers based on a discrete logarithm.

g. Levy, U.S. Patent No. 6,889,332 discloses verifying by a verifier that a prover has access to a private key associated to a public key comprising the prover generating a random number.

h. Liskov et al, U.S. Patent No. 6,411,715 disclose demonstrating that a public/private key pair is cryptographically strong.

i. Solinas, U.S. Patent No. 6,898,284 discloses generating a digital signature.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Wyszynski whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 5712723811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AHW

KAMBIZ ZAND
PRIMARY EXAMINER

KAMBIZ ZAND
PRIMARY EXAMINER